UCrypt® Q2IP

Patent Pending

UCrypt® Cable Gateways QAM to IP

QUICK START GUIDE

Although every effort has been taken to ensure the accuracy of this document it may be necessary, without notice, to make amendments or correct omissions. Specifications subject to change without notice.

TABLE OF CONTENTS

This page intentionally left blank

SAFETY

1. Safety

WARNING! FAILURE TO FOLLOW THE SAFETY PRECAUTIONS LISTED BELOW MAY RESULT IN PROPERTY DAMAGE OR PERSONAL INJURY. PLEASE READ AND COMPLY WITH THE FOLLOWING:

SAFETY GROUND: The connection to earth of the supplementary grounding conductor shall be in compliance with the appropriate rules for terminating bonding jumpers in Part V of Article 250 of the National Electrical Code, ANSI/NFPA 70, and Section 10 of Part I of the Canadian Electrical Code, Part I, CSA C22.1.

WATER AND MOISTURE: Care should be taken to prevent entry of splashed or dripping water, other liquids, and physical objects through enclosure openings.

DAMAGE: Do not operate the device if damage to any components is suspected.

POWER SOURCES: Only connect the unit to a power supply of the type and capacity specified in the operating instructions or as marked on the device.
> **NOTE:**   a) For 115 VAC operation, use the power cord supplied for operation from a 115 VAC source.
> b) For 230 VAC operation, use the power cord supplied for operation from a 230 VAC source.

GROUNDING OR POLARIZATION: Electrical grounding and polarization means must not be defeated.

POWER CORD PROTECTION: Care must be taken during installation to route or arrange the power supply cord to prevent and avoid the possibility of damage to the cord by external objects. Pay particular attention to the exit point from the device and plug.

POWER SUPPLY CORD ROUTING: The power supply cord shall not be attached to the building surface, nor run through walls, ceilings, floors and similar openings in the building structure.

SERVICE: Do not attempt to service the device beyond procedures provided the operating instructions. All other servicing should be referred to qualified service personnel.

MODIFICATIONS: Modifications should not be made to the device or any of its components for applications other than those specified in the operating instructions.

SAFETY CODES AND REGULATIONS: The device should be installed and operated in compliance with all applicable local safety by-laws, codes and regulations.

BATTERY REMOVAL AND REPLACEMENT: Disconnect power (AC or DC) from the equipment before battery removal and replacement. This is accomplished by unplugging the power cord from the power outlet. Replace the battery with Sony part No. CR2032 or exact replacement only.
> **CAUTION:**   Use of a different battery type may present a risk of fire or explosion.

BATTERY DISPOSAL: Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations. Please call 1-800-8-BATTERY or go to the website at www.call2recycle.org for information on recycling or disposing of your used battery.

This page intentionally left blank

QUICK START GUIDE – READ ME FIRST

2. Quick Start Guide – READ ME FIRST

For detailed information on configuration, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

This Quick Start Guide will take you through the steps required to get your UCrypt up and running if you have not done this before. Follow the steps below:

2.1 Install and Power Up

You may be doing this first setup in your lab so detailed installation details are not provided here. See the Installation and Operation Manual for installation details. You can get it from the ATX website (atxnetworks.com) in the Resource & Support section, User Documents sub-section. You will first need to get a user name and password from your ATX Networks support or sales representative and the contact numbers are on this same web page.

Refer to "Installation Summary" on page 4-1 for a brief overview of mounting and powering information.

> ⚠️ **NOTE:** If the unit is to be mounted in a rack, it is essential to attach the rear mounting ears to mounting rails to provide support or alternately install the equipment on a well supported shelf.

2.2 Plug in the CableCARD™ Modules

The CableCARD host slots are on the rear panel of the UCrypt for some versions or behind the front fan panel in the Version 2 model. CableCARD modules are hot swappable so they may be inserted or removed at any time. Depending on the ordered configuration, your UCrypt may have 1 to 10 active CableCARD slots. CableCARD modules may be inserted in any order.

> ⚠️ **NOTE:** Great care should be taken with the CableCARD modules to not forcibly insert them - the card should slide in and seat easily. Forcing the card into the slot is likely to result in bent pins in the PCMCIA host interface which will prevent proper operation of the UCrypt.

Refer to "Activating a CableCARD™ Module" on page 8-1 for instructions for activating CableCARD modules.

2.3 Connect the Cables

A PC with web browser and Ethernet network port will be required to configure the UCrypt. Establish a network connection with the supplied crossover network cable.

Connect QAM digital input signals to the input F fitting at a level of +5 to +10 dBmV per digital carrier.

Refer to "Cabling Connections" on page 5-1 for more details.

2.4 Start the Management Interface

The software for configuring the UCrypt Management Interface is provided by a built in secure web server which presents configuration pages. You will connect with the secure web server at **https://192.168.0.23** which is the default address, and log in to access the Interface.

The UCrypt will take about 90 seconds to boot up after applying power before you can begin configuration.

Refer to "Management Interface" on page 7-1 for basic setup instructions to connect to the Management Interface.

2.5 Change Network Settings

If it is necessary to change the network IP address to access this unit remotely on a network, that is done on the **System** tab.

Refer to "SYSTEM Tab - Configuration" on page 12-1 to change the IP addresses.

2.6 Pair the CableCARD™ with its Host

You will need to pair each CableCARD module with its host, that is, the Host Slot receptacle on the UCrypt. If this CableCARD is not a permanent CableCARD to be installed in this unit, pairing will need to be done again with the exact permanent CableCARD and host slot.

The process of pairing is required for security so the CableCARD may not be moved from the host that it is originally paired with and plugged in somewhere else. If it is moved, it will require the pairing operation to be done again with the new host and it will not decrypt any services until that is done.

The pairing information will be obtained from the Management Interface after you log in and will need to be passed to your Billing System Administrator who will setup an account and enter the pairing information.

Refer to "Activating a CableCARD™ Module" on page 8-1 for more details.

2.7 Optionally Import an Existing Configuration File

UCrypt supports mass deployment with an exportable configuration file. If you have a previously exported configuration file to import see "13. CONFIGURATION tab - Configuration" on page 13-1 for more details.

If you have no file to import skip to Step 2.8 below.

2.8 Select Programs for Decryption

After you have paired available CableCARD modules with the host receptacle slots, the UCrypt will receive a Channel Map and display available programs in a window. You should now select channels for decryption to test CableCARD validation and authorization. After each available CableCARD is verified to be working, continue selecting programs that will be needed for the final output lineup. Encrypted programs can be selected for decryption and programs that are in the clear may also be selected to passthrough to the output.

Refer to "CHANNEL VIEW Tab - Configuration" on page 9-1 for more details.

2.9 Review or Change CableCARD™ Configuration

After having selected programs for decryption, you may need to change settings or remove a program.

Refer to "CableCARD™ VIEW Tab - Configuration" on page 10-1 for more details.

2.10 Set up Output IP Streaming Addresses and Output Multiplexes

You will need to define the MPEG output IP addresses and assign programs to each address. There are three physical IP output ports and 8 IP addresses are assigned to each physical port so connect to the appropriate port to view the configured output streams. Note which program is routed to each specific physical port on the Output MPTS View tab.

Refer to "OUTPUT MPTS VIEW Tab - Configuration" on page 11-1 for more details.

That's it, you're done

You should have programs streaming from the IP output ports you configured.

If the programs are in the clear, you may use software on your PC such as VideoLAN (www.videolan.org) or use an appropriate decoder to view Pro:Idiom® encrypted programs.

Download the full Installation & Operation Manual from the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section for more details than are presented here. Click the **Help** tab to link to the manual or download it to your Management Computer.

IMPORTANT CONFIGURATION INFORMATION

3. Important Configuration Information

3.1 Support for Two Simultaneous Configurations

As work on configuration progresses, changes will need to be made to multiple pages in the Management Interface. As work is completed on each page, the changes must be saved and there is a **Save** button conveniently located on every configuration page where configuration changes can be made. If changes are made and you navigate away from the page without saving, the changes may be discarded.

When you are satisfied that all configuration changes on the UCrypt are complete and correct, click the **Apply** button located by the save buttons on any page, they all do the same thing. There is no need to apply the configuration as you complete work on each page. You may **Save** your work as you go and **Apply** the configuration when completed.

3.1.1 Saved Configuration

This can be thought of as a work in progress and any changes can be made in the configuration without affecting how the UCrypt is currently working and providing services.

This saved configuration can be discarded at any time without affecting the working UCrypt configuration or can be Applied to the UCrypt, to make it the new working configuration. To discard your configuration changes browse to the **Configuration** tab and click the **Revert** button. The Revert action is not service affecting.

3.1.2 Applied Configuration

This is the working configuration that the UCrypt is currently using to provide the desired services to the output and regardless of the changes made in the Management Interface as discussed above, changes do not take effect until the **Apply** button is clicked and the configuration is applied.

During configuration, while changes are being made, the saved configuration and the applied configuration differ by the changes that have been made and saved since last clicking **Apply**. After the Apply button is clicked, the saved configuration and the applied configuration are identical.

> **NOTE:** Clicking the Apply button will cause a service interruption while the UCrypt re-provisions itself with the new working configuration. It is best to make all changes necessary on all configuration pages and apply the changes when completed.

This page intentionally left blank

INSTALLATION SUMMARY

4. Installation Summary

4.1 Mounting

⚠️ **NOTE:** *If the UCrypt unit is to be mounted in a rack, it is essential to attach the rear mounting ears of the unit to rear mounting rails to provide support or alternately install the equipment on a well supported shelf*

Rack mount brackets are provided with the UCrypt for mounting in a standard EIA 19‰ rack. Brackets are also provided for mounting the UCrypt to a vertical backboard for sites where no rack mounting facilities exist.
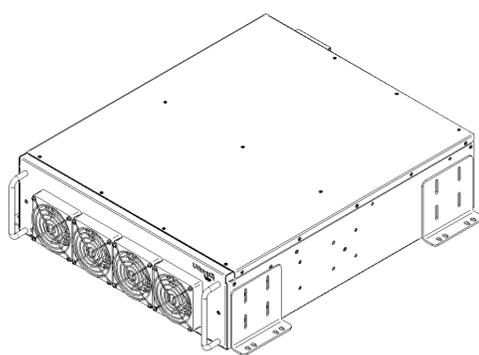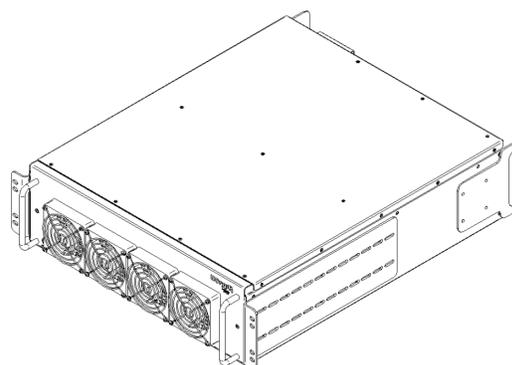
Panel Mount   Rack Mount

4.2 Equipment Safety Grounding

It is imperative that the UCrypt housing be connected to a permanent building ground in a manner that will ensure that the exposed metal parts are constantly connected to ground even when the power cord may be disconnected temporarily. A grounding lug is provided on the rear panel to conveniently effect such a connection. The following guidelines are provided to clarify the requirements for the installation to meet UL, CUL and CB standards. The use of the words "Ground" and "Earth" as well as "Grounding" and "Earthing" may be used interchangeably and in this context, have the same meaning.

1. The supplementary equipment grounding conductor is to be installed between the UCrypt rear panel ground connector and earth, that is, in addition to the equipment ground conductor in the power supply cord.

2. The supplementary equipment grounding conductor may not be smaller in size than the branch-circuit supply conductors or a minimum #14 AWG. The supplementary equipment grounding conductor is to be connected at the rear panel terminal provided, and connected to earth in a manner that will retain the earth connection when the power supply cord is unplugged. The connection to earth of the supplementary grounding conductor shall be in compliance with the appropriate rules for terminating bonding jumpers in Part V of Article 250 of the National Electrical Code, ANSI/NFPA 70, and Section 10 of Part I of the Canadian Electrical Code, Part I, CSA C22.1.

3. Termination of the supplementary equipment grounding conductor may be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment earth.

4. Bare, covered or insulated grounding conductors are acceptable. A covered or insulated grounding conductor shall have a continuous outer finish that is either green, or green with one or more yellow stripes.

4.3 Ambient Environment

The UCrypt is designed to operate to specification in an ambient room temperature of 0°C to +50°C (+32°F to +122°F) however it is recommended that it is installed in an environment that approximates normal room temperature to ensure proper long term operation.

4.4   Power Requirements

The UCrypt is designed with an autosensing switching type power supply which can operate on a wide range of input voltages from 115 VAC to 230 VAC. There is no need to configure the power supply to operate on any voltage in this range. The power cord provided with the UCrypt is a North American configuration with a NEMA 5-15 grounded plug for 115 VAC. If it is necessary to operate the UCrypt on 230 VAC, the installer must obtain an IEC cord with a NEMA 6-15 grounded plug for use in North America.

CABLING CONNECTIONS

5.   Cabling Connections

The input signal level presented to the UCrypt must be in the range of +5 to +10 dBmV per digital carrier as measured at the RF input port.

An Ethernet Cable is provided with the UCrypt for connecting to the Management Computer.

UCrypt® QAM to IP Rear Panel Connections
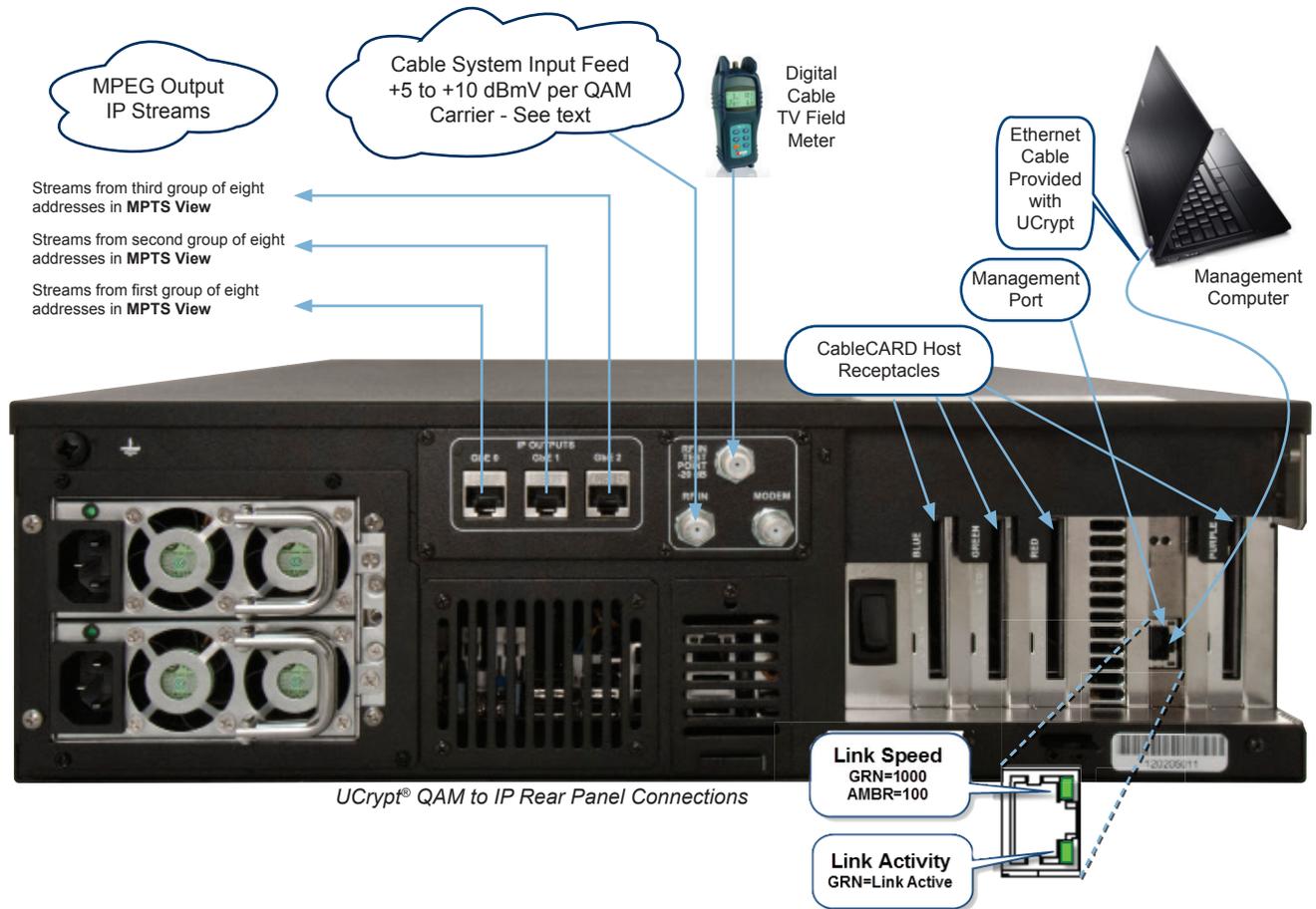
This page intentionally left blank

POWERING UP

6.   Powering Up

⚠️ **NOTE:** *The factory default configuration is that all IP output address ports are disabled so no unintended output into the distribution network is possible.*

If the UCrypt has been pre-provisioned elsewhere, before powering the UCrypt, ensure that the network output cables are disconnected from the distribution network to avoid unintentional service outages if there are overlaps between the IP output addresses of the UCrypt and existing services on the network.

Apply power and turn on the rear panel switch below the power receptacle. Boot-up of the UCrypt will take approximately 90 seconds.

This page intentionally left blank

MANAGEMENT INTERFACE

7. Management Interface

7.1 Connect to the Management Interface

Minimum Management Computer Requirements

- Computer running Windows® or other OS
- Ethernet Network port available
- Web browser such as Internet Explorer®, Firefox® or similar
- Adobe Reader for reading this manual
- Notepad or text editor for capturing text and logs

7.2 Configure the Management Computer Network Port

Set-up of the UCrypt unit requires a laptop or desktop PC running Microsoft® Windows or other operating system with an available Ethernet network port (called the Management Computer in the following procedures).

The Management Computer network port must be assigned an IP address in the same subnet as the UCrypt for access to the Management Interface. The following procedures are for Microsoft Windows XP and a factory default IP address setting on the UCrypt of 192.168.0.23 subnet 255.255.255.0

- Connect the Management Computer Ethernet adapter to the UCrypt Ethernet port using a Cat5e network cable (supplied with the unit). Link lights should illuminate indicating that the cable connection is correct and working.
- Set the Management Computer Ethernet interface to a static IP address on the 192.168.0.x subnet, as described below:
  - From the Control Panel, open Network Connections and select the connection associated with the Ethernet adapter to be used for connecting to the UCrypt (e.g., Local Area Connection).
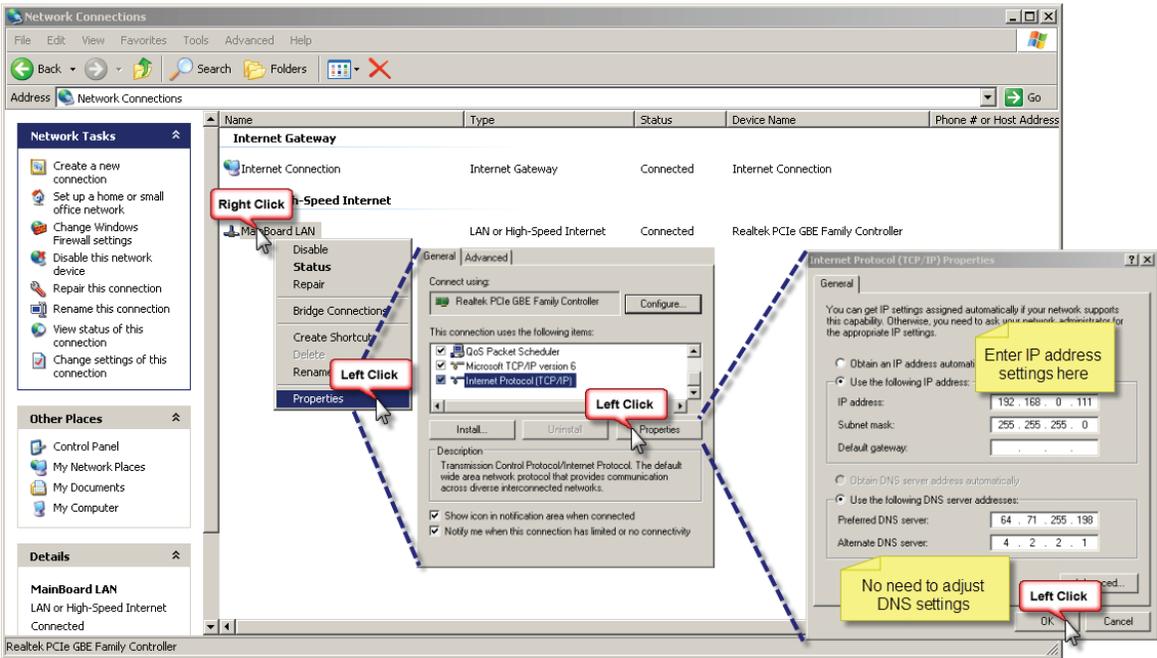
  - Right click on the connection and select Properties.
  - Select Internet Protocol (TCP/IP) and click Properties.
  - Click the selection box beside Use the following IP address to enter a check mark in the box.

- ◦   In the IP address field, enter 192.168.0.x (where x represents any number from 1-253 except 23).
- ◦   In the subnet mask field enter 255.255.255.0.
- ◦   Click OK and then OK again in the previous window.

7.3   Log in to the Management Interface

On the management computer, open a web browser and enter **https://192.168.0.23** in the address field.

If this is the first time you have connected to this UCrypt with this Management Computer, you may get a warning of a security violation or error. This is due to the UCrypt having a self signed security certificate and is not a security threat but your browser identifies it as such. Simply accept the security exception and proceed to the login screen as shown next. Other browsers will typically respond in the same manner.

Warning For Firefox Browser:
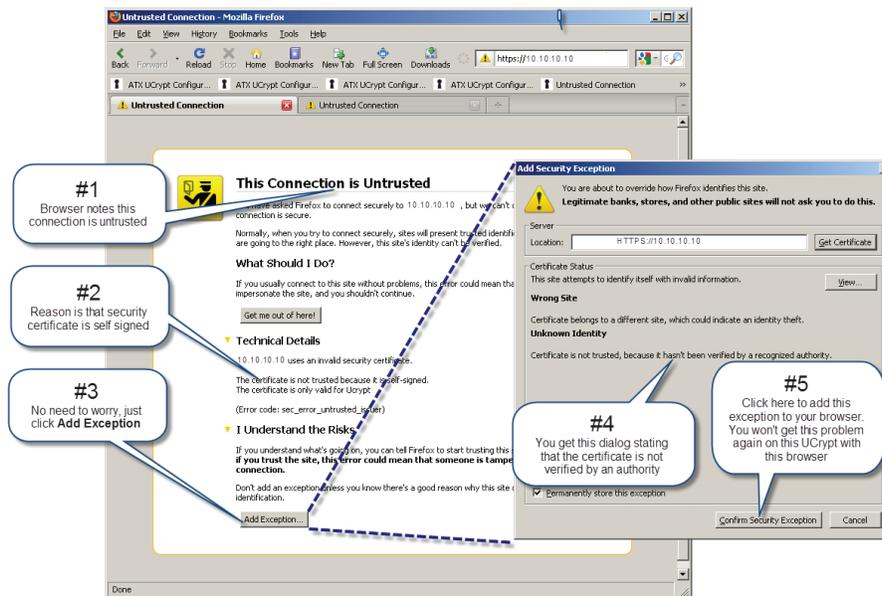
Warning For Internet Explorer:
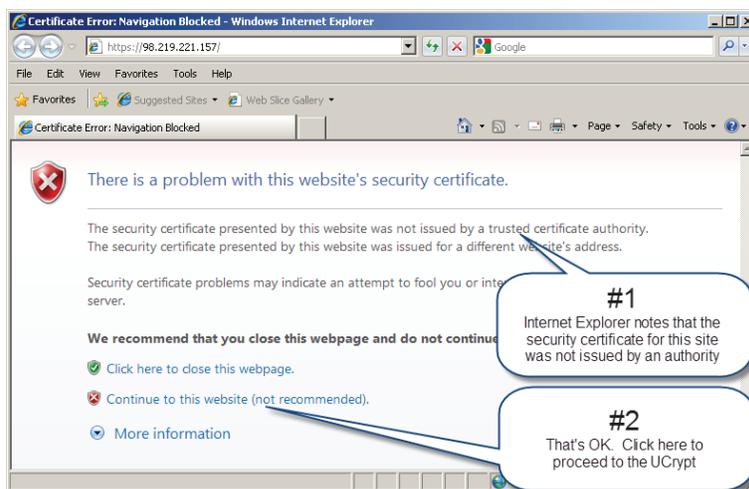
You should be presented with the following screen on the left, prompting you to log in:
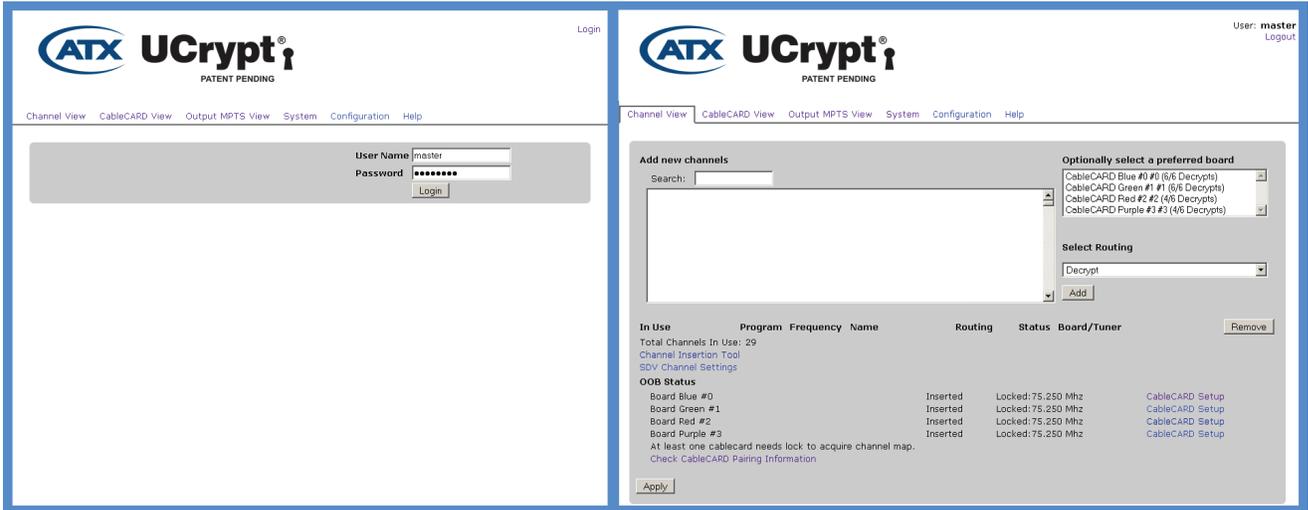
Default User Names, Passwords and Privileges				
Account User	Modify UCrypt® Settings	Install Updates	Set Passwords	Default Password
master	Yes	Yes	Yes	atx_ucrypt_master_password
admin	Yes	No	No	atx_ucrypt_admin_password
user	No	No	No	atx_ucrypt_user_password

Enter the appropriate **User Name** and **Password** for the access level you require for unit from the table above. The master user is the only user that can perform configuration.

When the login username and password are successfully entered, the screen on the right above will be presented.

This page intentionally left blank

ACTIVATING A CableCARD™ MODULE

8. Activating a CableCARD™ Module

Activate CableCARD modules by pairing them with the UCrypt host slots on the Channel View tab.

#1
Click here to select the Channel View page to begin CableCARD setup

#2
Plug CableCARDs into the host receptacles on the UCrypt rear panel. The UCrypt unit is equipped with four CableCARD slots that function as four individual hosts. CableCARD hosts are identified by the colors **blue, green, red and purple** both on the UCrypt back panel and in the Management Interface.
Be sure to fill the slots in that order if there are less than 4.

#7
CableCARD must show **Validated** after setup completes

#3
Check here to see that the OOB carrier has been aquired and is locked. This must be locked to continue.

#4
Click here to open a new window to see the CableCARD pairing information. This next page may take some time to load after CableCARD insertion due to firmware upgrades occuring.

Note:
CableCARD data for Moto is shown. SA/Cisco differs slightly but procedure is the same

#6
After CableCARD pairing information has been entered in the billing system and some time allowed for that information to be processed, click here to monitor the validation and authorization process for each CableCARD

#5
Use your mouse to click and hold while dragging across the data to highlight and copy this information to Notepad.

Alternately, you can copy the information manually.

Send this infomation to your billing system administartor.

Each host and CableCARD device must be set up as a valid pair in the billing system as a **"One-way Host"**.

This page intentionally left blank

CHANNEL VIEW TAB - CONFIGURATION

9. CHANNEL VIEW Tab - Configuration

Select programs from the system channel map for decryption on the Channel View tab.

![warning icon] **NOTE:** *Clicking the Apply button will cause a service interruption while the UCrypt re-provisions itself with the new working configuration. It is best to make all changes necessary on all configuration pages and apply the changes when completed.*

9.1 CableCARD™ Module Authorization Best Practice

When several CableCARD modules are inserted in the UCrypt, it is best to first route one program to each CableCARD to verify the validation and authorization of each. In step 4 of the illustration above, for the first programs being added, select a different CableCARD for each program until all CableCARD modules have at least one channel routed to them. If all of these programs decrypt, you can be sure of the authorization status and that they are working as they should.

If no specific CableCARD is selected in step 4, then the programs are added to the first CableCARD until full, then the second, and so on. The last CableCARD, if it has no programs routed to it initially, is left in doubt as to its true authorization status.

This page intentionally left blank

CableCARD™ VIEW TAB - CONFIGURATION

10. CABLECARD™ VIEW Tab - Configuration

Review and change CableCARD program decryption on the CableCARD View tab.

#1
To change configuration of the CableCARDs click **CableCARD View**

#2
Programs already selected and assigned previously on the **Channel View** page appear here. The frequency and constellation is automatically assigned by the UCrypt based on the multiplex properties when the first program is added to this CableCARD tuner

#3
Change a previously selected program decryption status here. This had been set earlier on the **Channel View** page.

Filter means drop the program.
Passthrough means pass a clear program through
Of course **Decrypt** means just that

#4
To remove this multiplex from the tuner click here, then click **Save** to remove the multiplex from being displayed on the screen

#5
Note that adding one program to a CableCARD, causes all other programs listed in the channel map on that multiplex to appear here, along with the added program, filtered by default

#6
Click **Save** button to save changes to the UCrypt until all changes are completed

NOTE: *Clicking the Apply button will cause a service interruption while the UCrypt re-provisions itself with the new working configuration. It is best to make all changes necessary on all configuration pages and apply the changes when completed.*

For detailed information on configuration of this page, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

This page intentionally left blank

OUTPUT MPTS VIEW TAB - CONFIGURATION

11. OUTPUT MPTS VIEW Tab - Configuration

Define streaming IP output addresses and multiplexes on the Output MPTS View tab.

![Warning icon] **NOTE:** *Clicking the Apply button will cause a service interruption while the UCrypt re-provisions itself with the new working configuration. It is best to make all changes necessary on all configuration pages and apply the changes when completed.*

For detailed information on configuration of this page, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

This page intentionally left blank

SYSTEM TAB - CONFIGURATION

12. SYSTEM Tab - Configuration

Access system wide properties on the System tab.

System Configuration Tab - Part 1

For detailed information on configuration of this page, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

System Configuration Tab - Part 2

For detailed information on configuration of this page, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

12.1 Users

Default Values				
Account User	Modify UCrypt® Settings	Install Updates	Set Passwords	Default Password
master	Yes	Yes	Yes	atx_ucrypt_master_password
admin	Yes	No	No	atx_ucrypt_admin_password
user	No	No	No	atx_ucrypt_user_password

CONFIGURATION TAB - CONFIGURATION

13. CONFIGURATION tab - Configuration

Access Mass Deployment and Backup file utilities on the Configuration tab.

NOTE: *Clicking the Apply button will cause a service interruption while the UCrypt re-provisions itself with the new working configuration. It is best to make all changes necessary on all configuration pages and apply the changes when completed.*

For detailed information on configuration of this page, go to the ATX website (atxnetworks.com) in the Resources & Support section, User Documents sub-section to download the Installation & Operation Manual.

This page intentionally left blank

SERVICE & SUPPORT

14. Service & Support

14.1 Contact ATX Networks

Please contact ATX Technical Support for assistance with any ATX products. Please contact ATX to obtain a valid RMA number for any ATX products that require service and are in or out-of-warranty before returning a failed module to ATX.

TECHNICAL SUPPORT

Tel: 289.204.7800 – press 1

Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: support@atx.com

SALES ASSISTANCE

Tel: 289.204.7800 – press 2

Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: insidesales@atx.com

FOR HELP WITH AN EXISTING ORDER

Tel: 289.204.7800 – press 3

Toll-Free: 866.YOUR.ATX (866.968.7289) USA & Canada only
Email: orders@atx.com
Web: www.atx.com

14.2 Warranty Information

All of ATX Networks' products have a 1-year warranty that covers manufacturer's defects or failures.

ATX Networks

Tel: 289.204.7800 | Toll-Free: 866.YOUR.ATX (866.968.7289) | support@atx.com

www.atx.com